09/844,693

REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is made obvious under the provisions of 35 U.S.C. §103. Thus, the Applicants believe that all of these claims are now in allowable form.

In addition, the Applicants' representative would like to thank Examiner Patel for kindly taking a substantial amount of time on February 20, 2008 to discuss the merits of the subject invention. The Applicants' representative is aware of the time constraint that is placed on the Examiner and is appreciative of the Examiner's willingness to devote such large quantity of time to discuss the case on the merits.

I. REJECTION OF CLAIMS 1, 3-6, 8-18, 20-23, 25-35, 37-40 AND 42-51 UNDER 35 U.S.C. §103

Claims 1, 3-6, 8-18, 20-23, 25-35, 37-40 and 42-51 stand rejected as being unpatentable over the Bots et al. patent (United States Patent No. 6,226,748, issued May 1, 2001, hereinafter "Bots") in view of the Pandya et al. patent (United States Patent No. 6,671,724, issued December 30, 2003, hereinafter "Pandya") and further in view of the Li patent (United States Patent No. 6,751,220, issued June 15, 2004, hereinafter "Li"). The Applicants respectfully traverse the rejection.

Particularly, the Examiner's attention is directed to the fact that Bots, Pandya, and Li, singly or in any permissible combination, fail to disclose or suggest a virtual private network (VPN) in which master nodes control admission and departure in the VPN for an associated non-empty subset of member nodes and perform membership changes in associated subsets without notifying all of the other master nodes of the change, as claimed in Applicants' independent claims 1, 18 and 35.

By contrast, Bots teaches that "the VPN units [which the Examiner equates with "master nodes"] maintain lookup tables for identifying members of specific virtual private network groups" (Bots, column 6, lines 34-36). These lookup tables must be consistent from VPNU to VPNU in order for messages to be handled properly: "It is assumed that the lookup tables maintained by all of the VPN units are both consistent and coherent" (Bots, column 7, lines 63-65, emphasis added). If all VPNUs must have the same

10

09/844,693

global view of the network, then it is impossible for a VPNU to make a membership change without informing all of the other VPNUs. That is, when a VPNU makes a membership change, it must update the lookup table, thereby necessarily informing all of the other VPNUs of the membership change. In fact, if a VPNU made a membership change (for example, added a node to a VPN group) without notifying the other VPNUs of the change, it could jeopardize the ability of the other VPNUs to properly process packets within the changed group (for example, the other VPNUs would not know that data packets to/from the added node should be encrypted/compressed/authenticated in accordance with the rules for the group).

The passages of Bots that the Examiner cites to support the changing of membership without notifying all of the VPNUs at best generally describes the lookup tables that each of the VPNUs maintain (i.e., specifically that the lookup tables define the compression, encryption, and authentication rules to be applied to each VPN group). As described above, however, these lookup tables must be consistent from VPNU to VPNU in order for messages to be handled properly by the VPN architecture (and, therefore, each VPNU must inform all other VPNUs of membership changes to maintain this consistency). This is explicitly supported by the disclosure of Bots (i.e., at least at column 7, lines 63-65, as provided above). Moreover, nothing in the passages of Bots that the Examiner cites teaches or suggests otherwise. In fact, the cited passages are completely silent with respect to the manner in which membership changes are addressed between VPNUs. Therefore, the cited passages of Bots cannot teach that a membership change in at least one of the VPN groups is performed without notifying all of the VPNUs not associated with the changed VPN group, as the Examiner suggests.

Notably, the Applicants positively claim master nodes that control admission and departure in a VPN for an associated non-empty subset of member nodes and that perform a membership change in an associated subset without notifying all of the other master nodes of the change, as claimed in Applicants' independent claims 1, 18 and 35. Specifically, Applicants' claims 1, 18 and 35 positively recite:

11

09/844,693

1. A group management system comprising:

a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted by said interconnected nodes; and

a plurality of master nodes, different from the plurality of interconnected nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes, <u>wherein a membership change in at least one of the subsets is performed without notifying all of the master nodes not associated with the changed subset</u>. (Emphasis added)

18. A method for managing a group, the method comprising:

providing a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted by said interconnected nodes; and

providing a plurality of master nodes, different from the plurality of interconnected nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes, <u>wherein a membership change in at least one of the subsets is performed without notifying all of the master nodes not associated with the changed subset</u>. (Emphasis added)

35. A computer readable medium containing an executable program for managing a group, where the program performs the steps of:

providing a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted by said interconnected nodes; and

providing a plurality of master nodes, different from the plurality of interconnected nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the

12

09/844,693

associated subset of member nodes will be automatically reassigned to one or more other of the master nodes,
     <u>wherein a membership change in at least one of the subsets is performed without notifying all of the master nodes not associated with the changed subset.</u> (Emphasis added)

Thus, the Applicants positively claim that a master node <u>performs a membership change in an associated subset of member nodes without notifying all of the other master nodes of the change</u>. As described above, Bots, Pandya, and Li, singly or in any permissible combination, fail to teach or suggest a mechanism by which a master node can perform a membership change in an associated subset of member <u>without notifying all of the other master nodes of the change</u>, but rather teaches that the equivalents of "master nodes" must share a <u>globally consistent view of network membership</u> in order for network communications to operate properly.

Bots, Pandya, and Li thus fail to teach or suggest a virtual private network (VPN) in which master nodes control admission and departure in the VPN for an associated non-empty subset of member nodes and <u>perform membership changes in associated subsets without notifying all of the other master nodes of the change</u>, as positively claimed by the Applicants in claims 1, 18 and 35. Therefore, for at least the reasons set forth above, the Applicants submit that independent claims 1, 18 and 35 fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claims 3-6, 8-17, 20-23, 25-34, 37-40 and 42-51 depend from claims 1, 18 and 35 and recite additional features therefore. As such, and for at least the reasons set forth above, the Applicants submit that claims 3-6, 8-17, 20-23, 25-34, 37-40 and 42-51 are not made obvious by the teachings of Bots in view of Pandya and further in view of Li. Therefore, the Applicants submit that dependent claims 3-6, 8-17, 20-23, 25-34, 37-40 and 42-51 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

09/844,693

II. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §103. Consequently, the Applicants believe that all of the presented claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.
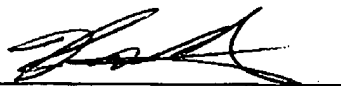
If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone <u>Mr. Kin-Wah Tong, Esq.</u> at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

_____2/21/08_____
Date

_____
Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702

14